

П Р А В О

УДК 34.05

ЗАРУБЕЖНОЕ УГОЛОВНОЕ ЗАКОНОДАТЕЛЬСТВО О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (штата Техас, Эстонской Республики, Республики Беларусь, Украины, Республики Узбекистан, Азербайджанской Республики, Республики Казахстан, Китайской Народной Республики, Японии)

© 2012 г.

А.А. Петров

Нижегородский госуниверситет им. Н.И. Лобачевского

ugol@jur.unn.ru

Поступила в редакцию 04.04.2012

Освещается уголовное законодательство девяти зарубежных стран, предусматривающих наказания за преступления в сфере компьютерной информации.

Ключевые слова: зарубежное уголовное законодательство, преступления в сфере компьютерной информации.

При совершенствовании уголовного законодательства в Российской Федерации, направленного на борьбу с преступлениями в сфере компьютерной информации, на наш взгляд, необходимо учитывать законотворческий опыт зарубежных стран. Рассмотрим особенности уголовного законодательства ряда зарубежных государств, касающиеся как юридической техники, так и содержания соответствующих норм, предусматривающих уголовное законодательство за преступления, совершаемые в сфере компьютерной информации.

Обращает на себя внимание Уголовный кодекс штата Техас [1, с. 345–353], в котором, в отличие от Российского уголовного законодательства, законодатель даёт в специальной статье определения категорий. В главе 33 «Компьютерные преступления» (статья 33.01 «Определения») раскрываются следующие понятия: (1) «Иметь доступ», (2) «Общая сумма», (3) «Поставщик услуг связи», (4) «Компьютер», (5) «Компьютерная сеть», (6) «Компьютерная программа», (7) «Компьютерные услуги», (8) «Компьютерная система», (9) «Компьютерное программное обеспечение», (10) «Компьютерный вирус», (11) «Данные», (12) «Надлежащее согласие», (14) «Вред», (15) «Собственник», (16) Имущество».

Далее законодатель указывает на следующее преступление в статье 33.02: «Нарушение компьютерной безопасности». В эту главу также

включены статьи, называющие процессуальных субъектов: статья 33.03 «Защиты», статья 33.04 «Участие прокурора штата».

В уголовном кодексе штата Техас имеется специальная глава 33А, посвящённая «Преступлениям в сфере телекоммуникаций». В статье 33А.01 «Определения» законодатель раскрывает содержание следующих понятий: (1) «Контрафактное устройство доступа к телекоммуникациям». (2) «Контрафактное телекоммуникационное устройство». (3) «Поставить». (4) «Опубликовать». (5) «Телекоммуникация». (6) «Телекоммуникационное устройство доступа». (7) «Телекоммуникационное устройство». (8) «Телекоммуникационные услуги». (9) «Стоимость телекоммуникационных услуг, полученных или в отношении которых была совершена попытка их получить».

В этой главе предусмотрена уголовная ответственность за следующие преступления: статья 33А.02 «Несанкционированное пользование телекоммуникационными услугами», статья 33А.03 «Изготовление, владение или поставка незаконного телекоммуникационного устройства», статья 33А.04 «Хищение телекоммуникационных услуг», статья 33А.05 «Обнародование телекоммуникационного устройства доступа», а также указан процессуальный субъект в статье 33А.06 «Участие прокурора штата».

Все перечисленные преступления, расположенные в главах 33 и 33А относятся к разделу 7.1 «Посягательства против собственности».

В уголовном законодательстве стран Балтии, например Эстонской Республики [2, с. 246–250], в главе 14 «Преступления в сфере компьютерной информации и обработке данных» находятся: статья 268 «Компьютерное мошенничество», статья 269 «Уничтожение компьютерной информации или компьютерных программ», статья 270 «Компьютерный саботаж», статья 271 «Незаконное использование компьютеров, компьютерных систем или компьютерных сетей», статья 272 «Незаконное нарушение или блокирование связи в компьютерной сети», статья 273 «Заведомое распространение компьютерных вирусов», статья 274 «Передача защитных кодов», статья 275 «Представление учреждениям недостоверных данных», статья 276 «Незаконная выдача данных из государственного или муниципального банка данных».

В УК Республики Беларусь [3, 386–392] предусмотрено уголовное наказание в разделе 12 «Преступления против информационной безопасности», в главе 31 «Преступления против информационной безопасности», за преступления – в статьях: 349 «Несанкционированный доступ к компьютерной информации», 350 «Модификация компьютерной информации», 351 «Компьютерный саботаж», 352 «Неправомерное завладение компьютерной информацией», 353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети», 354 «Разработка, использование либо распространение вредоносных программ», 355 «Нарушение правил эксплуатации компьютерной системы или сети».

В УК Украины [4, с. 161–162], в разделе 16 «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей» предусматривается уголовная ответственность в статьях: 361 «Незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных систем», 362 «Хищение, присвоение, требование компьютерной информации или завладение ею путём мошенничества либо злоупотребления служебным положением», 363 «Нарушение правил эксплуатации автоматизированных электронно-вычислительных систем».

В УК Республики Узбекистан [5, с. 198–199] в главе 11 «Преступления, не связанные с хищением чужого имущества», в статье: 174 «Нарушение правил информатизации» в двух её частях предусмотрено наказание за различные преступления в сфере компьютерной информации: ч. 1. «Нарушение правил информатизации, то есть несанкционированный доступ в инфор-

мационные сети или санкционированный доступ в такие сети без принятия необходимых мер защиты, или незаконное получение из них информации, а равно умышленное изменение, утрата, изъятие или уничтожение информации при санкционированной работе с информационной системой, повлекшее значительный ущерб»; ч. 2 «Создание компьютерных вирусов или программ и их распространение без соответствующей санкции с целью изменения данных или программ, хранящихся в компьютерных системах, а равно несанкционированный доступ в информационную систему, повлекший искажение, изъятие, уничтожение информации или прекращение функционирования этой системы».

В УК Азербайджанской республики [6, с. 284–286], в главе 30 «Преступления в сфере компьютерной информации» предусматривается наказание за: «Неправомерный доступ к компьютерной информации» (ст. 271), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 272), «Нарушение правил эксплуатации электронно-вычислительных машин (ЭВМ), системы ЭВМ или их сети» (ст. 273).

В УК Республики Казахстан [7, с. 254–256], в главе 7 «Преступления в сфере экономической деятельности», в одной статье 227 законодатель установил ответственность за «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ».

УК Китайской Народной Республики [8, с. 108–112] в главе 6 «Преступления против порядка общественного управления», в §1 «Преступления против общественного порядка», в статьях 285, 286, 287 без названия предусматривает уголовную ответственность за преступления, связанные с компьютерной информацией.

Наказание предусмотрено за: «Незаконное вторжение в компьютерные информационные системы, имеющие отношение к новейшим научно-техническим разработкам, к строительству системы государственной безопасности и государственным делам» (ст. 285), (ч. 1) «Незаконное совершение с компьютерными информационными системами таких действий, как сокращение (изъятие) текста, исправление, дополнение, создание помех, приведшее к невозможности нормального функционирования компьютерной информационной системы, если это повлекло серьёзные последствия», (ч. 2) «Незаконное совершение с передаточными, оперативными и хранящимися в базе данными компьютерных информационных систем таких действий, как сокращение, исправление, дополнение, повлекшее серьёзные последствия», (ч. 3)

«Умышленное создание и распространение компьютерных вирусов и иных программ деструктивного характера, оказывающих влияние на нормальное функционирование компьютерных систем, повлекшее серьёзные последствия» (ст. 286), «Использование компьютера для завладения деньгами путём мошенничества или их хищения, для взяточничества и нецелевого использования общественных средств, для завладения путём хищения государственной тайной и совершения иных преступлений» (ст. 287).

В УК Японии [9, с. 72–77] в главе 35 «Преступления против кредита и профессиональной деятельности» предусматривается наказание за «Препятствование выполнению профессиональной деятельности путём повреждения ЭВМ или другим способом» (234-II) и в главе 37 «Преступления, состоящие в мошенничестве и вымогательстве» предусматривается наказание за «Противоправное извлечение выгоды путём изготовления электромагнитной записи, противоречащей истине».

Приведенные нормативные акты отличаются при регламентации преступлений в сфере компьютерной информации как по форме, так и по содержанию. Различия состоят прежде всего в расположении соответствующих статей в разделах и главах уголовных кодексов зарубежных стран, имеющих свои названия, а в УК штата Техас и в УК Японии они размещены в ряде глав. Кроме того, в УК штата Техас имеются две самостоятельные главы, посвященные: 33 «Компьютерным преступлениям» и 33 А «Преступлениям в сфере телекоммуникаций», а в главе 16 УК штата Техас законодатель регламентирует «Преступный инструментарий, перехват телеграфного или устного сообщения и установление устройства обнаружения». Существует отличие в количестве статей и преступлений, предусмотренных этими статьями. Например, в УК Республики Узбекистан имеется только ст. 174, а в УК Республики Казахстан – ст. 227, в которых законодатель в соответствующих частях предусматривает наказание за самостоятельные преступления. В УК Китайской Народной Республики статьи имеют только номер, но не имеют названия, а наказание за преступления, указанные в ч. 2 и 3, находится в ч. 1 ст. 286.

По-разному в уголовном законодательстве зарубежных стран раскрываются объективные и

субъективные признаки составов преступлений в сфере компьютерной информации. Квалифицирующие признаки преступлений в сфере компьютерной информации имеются не во всех уголовных кодексах зарубежных стран. Квалифицирующие признаки в различных уголовных кодексах зарубежных стран характеризуют как объективную и субъективную стороны составов преступлений в сфере компьютерной информации, так и субъекта.

Список литературы

1. Уголовный кодекс штата Техас / Научное редактирование и предисловие канд. юрид. наук, проф. И.Д. Козочкина. Перевод с английского Д.Г. Осипова, И.Д. Козочкина. СПб.: Изд-во Р. Асланова «Юридический центр Пресс», 2006. 576 с.
2. Уголовный кодекс Эстонской Республики / Науч. ред. и перевод с эстонского В.В. Запелавова. Вступ. статья канд. юрид. наук, доц. СПбГУ Н.И. Мацнева. СПб.: Изд-во «Юридический центр Пресс», 2001. 262 с.
3. Уголовный кодекс Республики Беларусь / Принят Палатой представителей 2 июня 1999 года. Одобрен Советом Республики 24 июня 1999 года / Предисловие проф. Б.В. Волженкина; Обзорная статья А.В. Баркова. СПб.: Изд-во «Юридический центр Пресс», 2001. 474 с.
4. Уголовный кодекс Украины. Симферополь: Реноме, 2001. 224 с.
5. Уголовный кодекс Республики Узбекистан (с изменениями и дополнениями на 15 июля 2001 г.) / Вступительная статья М.Х. Рустамбаева, А.С. Якубова, З.Х. Гулямова. СПб.: Изд-во «Юридический центр Пресс», 2001. 338 с.
6. Уголовный кодекс Азербайджанской Республики / Научное редактирование, предисловие докт. юрид. наук, проф. И.М. Рагимова. Перевод с азербайджанского Б.Э. Аббасова. СПб.: Изд-во «Юридический центр Пресс», 2001. 25 с.
7. Уголовный кодекс Республики Казахстан / Закон Республики Казахстан от 16 июля 1997 года № 167 (Ведомости Парламента РК, 1997 г., № 15–16, ст. 211) / Предисловие министра юстиции Республики Казахстан, докт. юрид. наук, проф. И.И. Рогова. СПб.: Изд-во «Юридический центр Пресс», 2001. 466 с.
8. Уголовный кодекс Китайской Народной Республики / Под ред. и с предисл. проф. А.И. Коробеева. Пер. с кит. Владивосток: Изд-во Дальневост. ун-та, 1999. 176 с.
9. Уголовный кодекс Японии / Под ред. и с предисл. проф. А.И. Коробеева. Пер. с япон. Владивосток: Изд-во Дальневост. ун-та, 2000. 84 с.

FOREIGN CRIMINAL LAW ON CYBERCRIME (State of Texas, Republic of Estonia, Republic of Belarus, Ukraine, Uzbekistan, Azerbaijan Republic, Republic of Kazakhstan, People's Republic of China, Japan)

A.A. Petrov

The article highlights criminal law of nine foreign countries providing for penalties for crimes in the sphere of computer information.

Keywords: foreign criminal law, cybercrime.